Why General Counsel should care about Software Asset Management

An organization’s ability to maintain compliance with its contractual obligations and manage costs depends on whether or not it has the formal governance, people, process and technology in place to effectively manage software. While organizations have long understood the need to manage hardware assets (e.g., servers, laptops/desktops, printers, etc.) to contain costs, similar diligence for software assets has lagged. Software is viewed as a less tangible asset which, given its perceived pseudo-physicality, makes it more challenging to track and maintain control over its deployment and use throughout an organization. Despite these challenges, organizations that effectively manage software through a Software Asset Management (“SAM”) program not only reduce their risk of exposure to noncompliance findings resulting from an audit, but are able to achieve ongoing benefits such as, but not limited to: cost savings achieved through taking full advantage of volume licensing programs, reusing licenses, and avoiding redundant software purchase and shelf-ware (i.e., software purchased, but never installed); optimizing IT; improving vendor relationships; and enhancing security.

General Counsel are often not involved in the initial negotiation of software license agreements, which we believe is a missed opportunity. Software license agreements can be complex and may include specific technical language which may not be clearly defined nor well understood outside of the IT world. Certain legal, IT, and technical terms are often embedded into these agreements, and these terms and conditions are often negotiated directly by IT or procurement, with minimal involvement from legal. In addition, software publishers offer dramatically different types of contractual agreements and licensing metrics associated with their products—there is no “one size fits all” agreement. As the software industry continues to consolidate, many legacy agreements are not assigned or transferred in a timely manner, exposing organizations to unnecessary risks.

Increasingly, software publishers are executing their contractual right to audit customers under existing software license agreements to protect their IP as well as to recover any revenue from under and mis-licensed software. Collections from noncompliance may include payment for licenses and back support as a true-up payment for under-licensed software titles as well as reinstatement penalties which can lead to significant unbudgeted expenses ranging from thousands to millions of dollars. However, an
organization’s true cost of noncompliance with the terms and conditions of existing software license agreements goes beyond the settlement with the software publisher upon conclusion of the audit. An organization’s true cost considers the resources and time committed to respond to the audit, level of disruption to the business and impact on the customer-vendor relationship in addition to the actual noncompliance settlement expense.

Software audits are on the rise

While software license compliance programs are a part of good corporate governance and have been in place for years at software publishers throughout the industry, the number and frequency of software audits conducted by software publishers at their customers is on the rise. Software publishers are aggressively protecting their IP as well as recovering lost revenue from under and mis-licensed software. Noncompliance findings can vary widely based on a number of different factors including the type of software (i.e., server, client, developer, etc.), amount of software deployed within the customer’s organization, and the scope of audit (i.e., geographies, software titles, etc.). Findings resulting from software audits can range from non-monetary issues such as failure to execute administrative tasks (e.g., neglecting to complete required license transfer documentation after a migration to a new data center) to monetary findings ranging from thousands to millions of dollars.

Noncompliance is typically not the result of intentional mis-use or illegal actions among organizations, as is the case of piracy, but rather a lack of governance, people, process and technology in place to properly manage software and their associated license agreements. License agreements vary across software publishers, and terms and conditions within agreements need to be understood by stakeholders not only within IT, but procurement, vendor management, compliance, legal, internal audit and the business units to ensure an organization’s ability to maintain compliance over time. A disconnect between the terms and conditions defined in the agreement with the organization’s ability to track, meter and monitor software licenses can lead to an increased risk of noncompliance. This may not be an issue of how the terms were originally defined in an agreement, but may be the consequence of factors such as: changes in corporate structures resulting from acquisitions and divestitures, evolving business needs impacting the software’s usage, and advances in technology. For example, advances in technology such as virtualization allowing organizations to optimize IT environments by providing increased computing power with less physical hardware (among other potential benefits), may not have been contemplated at the time a software product was purchased, but nevertheless may impact how an organization needs to track and measure license usage for the software product in a virtualized environment. Legal is often consulted to provide an interpretation of the organization’s obligations in such circumstances, but all too often the discussion occurs during the midst of a software audit and not as a part of routine process to effectively manage software assets.

Measuring compliance requires the monitoring of a software product’s license position consisting of the license entitlement as well as the deployment and/or usage of the software. License entitlement information resides within the terms of software license agreements, purchase documents and other use rights documents published by the software publisher. This information is commonly maintained in different forms between vendor management, procurement, IT and legal functions, but the challenge for organizations is in sharing this information in a way that allows for an accurate snapshot of entitlement as well as mechanisms to track their entitlement position over time. This task is complicated by the diverse set of license metrics on which software publishers license their products.

Common license metrics include (to list a few): per seat/device, per user, per concurrent user, per processor and per processor value unit (“PU”), but many software titles have additional restrictions associated with their usage that adds elements of complexity to the tracking and monitoring of software across an organization. Restrictions may include: geography, environment (i.e., physical and virtual), hardware specifications (e.g., maximum # of possible physical processors), system tiering classifications (i.e., the concept of classifying specific hardware into groups to differentiate license cost), and type of usage (i.e., production, test and development). Tracking these license metrics, and information regarding the restrictions on usage, requires not only a network discovery tool capable of scanning hardware for the existence of the software and collecting device specifications (e.g., system make and model, processor and core counts, etc.), but information about the system architecture (e.g., physical and virtual environment attributes) and end-user usage (e.g., location

---

1 “Survey Analysis: Survey Shows Another Increase in Software Vendor Audits; IT Asset Managers Should Prepare Now” 2 March 2011 and “Gartner Polls and Surveys Show an Increase in Software License Audits” 31 July 2009

PwC Why General Counsel should care about Software Asset Management
of software users, type of usage, etc.) to be collected from IT environments. Organizations that are able to effectively inventory and reconcile license entitlement with deployment and usage are better positioned to maintain compliance with the contractual obligations of their software license agreements, realize cost savings, optimize IT, improve vendor relationships and enhance security. This can be done and positioned through executing on formalized processes within a well-defined SAM program, and not as a result of ad-hoc “heroic” efforts of personnel during an audit.

An understandable definition of SAM

SAM has been defined by the Information Technology Infrastructure Library (“ITIL”) as “... all of the infrastructure and processes necessary for the effective management, control, and protection of the software assets within an organization, throughout all stages of their lifecycle.” Organizations that implement sound SAM practices are able to achieve the benefits, which are not limited to:

- **Cost Savings:** Managing software assets in real-time leads to cost savings from:
  - Taking full advantage of discounts offered by software vendors through volume licensing programs;
  - An increased capability to reuse, or “harvest”, software licenses by re-deploying software from retired or repurposed hardware assets;
  - Reducing the over purchasing of software licenses and support by knowing exactly what is required by the business as well as avoiding software becoming shelf-ware; and
  - Eliminating purchases of redundant applications where different software titles providing similar functionality to the business are offered by competing software publishers.

- **IT Optimization:** Improving the organization’s ability to request, procure, deploy, maintain and retire software licenses will allow IT to meet the needs of the business as well as drive accountability and accurately allocate costs;

- **Maintaining Compliance:** Accurately tracking and monitoring the procurement, deployment and use of software will allow the organization to maintain compliance with the legal obligations within the numerous software contracts;

- **Value-added Vendor Relationships:** Pro-actively managing software vendor relationships will lead to better communication and ability for software vendors to be more responsive to the needs of the business; and

- **Security:** Software not approved by the organization’s IT security team may expose the organization to a variety of risks including the loss of network connectivity, and possible exposure of confidential and sensitive information through malicious malware, viruses and worms.

To provide organizations with a set of international standards aimed at addressing corporate governance requirements and support for IT Service Management (“ITSM”), the International Organization for Standardization (“ISO”) and the International Electrotechnical Commission (“IEC”) have published ISO/IEC 19770-1:2006 “Information Technology—Software Asset Management—Part 1: Processes”. The standard provides a baseline set of processes for organizations to implement, but many organizations seek assistance from consultancies, solution-based product vendors, and software publishers. SAM specialists can provide organizations with help in applying industry leading practices, defining critical success factors, tracking key performance indicators, and designing roadmaps with specific policy and process design and implementation for a successful SAM program. Whether or not an organization decides external help is necessary, only effective SAM practices will be able to mitigate risk and reduce exposure to noncompliance risk with existing software license agreements.

Early involvement leads to optimal results

General Counsel have an opportunity to add value to the organization by being involved in the management of software throughout the lifecycle, beginning with the review and negotiations in executing a software license agreement. All too often, General Counsel’s first in-depth review of agreements occurs when a software publisher exercises their right to audit. During an audit, legal can assist in defining the scope of the audit (e.g., geographies, business units, software titles, etc.), ensuring the proper confidentiality agreements are in place, and providing legal interpretations of contractual obligations, but many of the noncompliance findings may be avoided by clearly defining terms of the

---

"An understandable definition of SAM" by PwC

---

2 ITIL’s Guide to Software Asset Management

PwC Why General Counsels should care about Software Asset Management 4
agreement at the execution of the agreement, and pro-active software management. Organizations that implement a SAM program to effectively manage software throughout the software asset lifecycle are able to maintain compliance with existing license agreements. Such organizations benefit by realizing cost savings, optimizing IT, improving vendor relationships, and enhancing security. Those organizations without the formal governance, people, process and technology in place will continue to be challenged with being able to efficiently respond to software audits and risk potentially significant un-budgeted expenses in the form of noncompliance true-up settlement payments to software publishers.

Contacts

To have a deeper conversation about how this subject may affect your business, please contact:

David Marston
PwC
(408) 817-3803
david.l.marston@us.pwc.com

Bruce Vanderbush
PwC
(415) 498-6595
bruce.a.vanderbush@us.pwc.com